特 許 協 力 条 約

発信人　日本国特許庁（国際予備審査機関）

Int'l Prel. Report on Patentability

代理人

新居　広守

様

あて名
〒532-0011
大阪府大阪市淀川区西中島３丁目１１番２６号
新大阪末広センタービル３Ｆ
新居国際特許事務所内

ＰＣＴ

特許性に関する国際予備報告（特許協力条約第二章）の送付の通知書

（法施行規則第 57 条）
〔ＰＣＴ規則 71.1〕

発送日 （日.月.年）	１１．０４．２００６
出願人又は代理人 の書類記号　P36663-P0	重要な通知

国際出願番号 ＰＣＴ／ＪＰ２００４／０１８４９１	国際出願日 （日.月.年）　１０．１２．２００４	優先日 （日.月.年）　１１．１２．２００３

出願人（氏名又は名称）
松下電器産業株式会社

１．国際予備審査機関は、この国際出願に関して特許性に関する国際予備報告及び付属書類が作成されている場合には、それらをこの送付書とともに送付することを、出願人に通知する。

２．国際予備報告及び付属書類が作成されている場合には、すべての選択官庁に通知するために、それらの写しを国際事務局に送付する。

３．選択官庁から要求があったときは、国際事務局は国際予備報告（付属書類を除く）の英語の翻訳文を作成し、それをその選択官庁に送付する。

４．注　意

出願人は、各選択官庁に対し優先日から３０月以内に（官庁によってはもっと遅く）所定の手続（翻訳文の提出及び国内手数料の支払い）をしなければならない（ＰＣＴ39条（１））（様式ＰＣＴ／ＩＢ／３０１とともに国際事務局から送付された注を参照）。

国際出願の翻訳文が選択官庁に提出された場合には、その翻訳文は、特許性に関する国際予備報告の付属書類の翻訳文を含まなければならない。この翻訳文を作成し、関係する選択官庁に直接送付するのは出願人の責任である。

選択官庁が適用する期間及び要件の詳細については、ＰＣＴ出願人の手引き第Ⅱ巻を参照すること。

出願人はＰＣＴ第 33 条(5)に注意する。すなわち、ＰＣＴ第 33 条(2)から(4)までに規定する新規性、進歩性及び産業上利用可能性の基準は国際予備審査にのみ用いるものであり、締約国は、請求の範囲に記載されている発明が自国において特許を受けることができる発明であるかどうかを決定するに当たっては、追加の又は異なる基準を適用することができる（ＰＣＴ第 27 条(5)も併せて参照）。そのような追加の基準は、例えば、実施可能要件や特許請求の範囲の明確性又は裏付け要件を、特許要件から免除することも含む。

名称及びあて名 日本国特許庁（ＩＰＥＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	権限のある職員 特　許　庁　長　官 電話番号　０３－３５８１－１１０１　内線　３５９６	５Ｘ　９０７７

様式ＰＣＴ／ＩＰＥＡ／４１６（２００４年１月）　　添付用紙の注意書きを参照

ATTACHMENT K

注　　意

1．文献の写しの請求について
国際予備審査報告に記載された文献であって国際調査報告に記載されていない文献の複写

特許庁にこれらの引用文献の写しを請求することもできますが、独立行政法人工業所有権情報・研修館（特許庁庁舎２階）で公報類の閲覧・複写および公報以外の文献複写等の取り扱いをしています。

〔担当及び照会先〕
〒１００－００１３　東京都千代田区霞が関３丁目４番３号（特許庁庁舎２階）
独立行政法人工業所有権情報・研修館
【公 報 類】　閲覧部　ＴＥＬ　03－3581－1101　内線3811～2
【公報以外】　資料部　ＴＥＬ　03－3581－1101　内線3831～3

また、（財）日本特許情報機構でも取り扱いをしています。
これらの引用文献の複写を請求する場合は下記の点に注意してください。

〔申込方法〕
（１）特許（実用新案・意匠）公報については、下記の点を明記してください。
○特許・実用新案及び意匠の種類
○出願公告又は出願公開の年次及び番号（又は特許番号、登録番号）
○必要部数
（２）公報以外の文献の場合は、下記の点に注意してください。
○国際予備審査報告の写しを添付してください（返却します）。
〔申込み及び照会先〕
〒１３５－００１６　東京都江東区東陽４－１－７　佐藤ビル
財団法人　日本特許情報機構　情報処理部業務課
ＴＥＬ　０３－３５０８－２３１３
注）　特許庁に対して文献の写しの請求をすることができる期間は、国際出願日から７年です。

2．各選択官庁に対し、国際出願の写し（既に国際事務局から送達されている場合は除く）及びその所定の翻訳文を提出し、国内手数料を支払うことが必要となります。その期限については各国ごとに異なりますので注意してください。（条約第22条、第39条及び第64条(2)(a)(i)参照）

特 許 協 力 条 約

PCT

特許性に関する国際予備報告（特許協力条約第二章）

（法第12条、法施行規則第56条）
〔ＰＣＴ36条及びＰＣＴ規則70〕

出願人又は代理人の書類記号　P36663-P0	今後の手続きについては、様式ＰＣＴ／ＩＰＥＡ／４１６を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ２００４／０１８４９１	国際出願日（日．月．年）　１０．１２．２００４	優先日（日．月．年）　１１．１２．２００３
国際特許分類（ＩＰＣ） Int.Cl. *H04L9/36 (2006.01), H04N7/167 (2006.01)*		
出願人（氏名又は名称） 松下電器産業株式会社		

1．この報告書は、ＰＣＴ35条に基づきこの国際予備審査機関で作成された国際予備審査報告である。
法施行規則第57条（ＰＣＴ36条）の規定に従い送付する。

2．この国際予備審査報告は、この表紙を含めて全部で　3　ページからなる。

3．この報告には次の附属物件も添付されている。

a．☑ 附属書類は全部で　１２　ページである。

☑ 補正されて、この報告の基礎とされた及び／又はこの国際予備審査機関が認めた訂正を含む明細書、請求の範囲及び／又は図面の用紙（ＰＣＴ規則70.16及び実施細則第607号参照）

☐ 第Ｉ欄４．及び補充欄に示したように、出願時における国際出願の開示の範囲を超えた補正を含むものとこの国際予備審査機関が認定した差替え用紙

b．☐ 電子媒体は全部で　　（電子媒体の種類、数を示す）。
配列表に関する補充欄に示すように、電子形式による配列表又は配列表に関連するテーブルを含む。
（実施細則第802号参照）

4．この国際予備審査報告は、次の内容を含む。

☑ 第Ｉ欄　国際予備審査報告の基礎
☐ 第Ⅱ欄　優先権
☐ 第Ⅲ欄　新規性、進歩性又は産業上の利用可能性についての国際予備審査報告の不作成
☐ 第Ⅳ欄　発明の単一性の欠如
☑ 第Ｖ欄　ＰＣＴ35条(2)に規定する新規性、進歩性又は産業上の利用可能性についての見解、それを裏付けるための文献及び説明
☐ 第Ⅵ欄　ある種の引用文献
☐ 第Ⅶ欄　国際出願の不備
☐ 第Ⅷ欄　国際出願に対する意見

国際予備審査の請求書を受理した日 ２０．０９．２００５	国際予備審査報告を作成した日 ２８．０３．２００６
名称及びあて先 日本国特許庁（ＩＰＥＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｘ　９０７７ 吉田　隆之 電話番号　０３－３５８１－１１０１　内線　３５９６

様式ＰＣＴ／ＩＰＥＡ／４０９（表紙）（２００５年４月）

特許性に関する国際予備報告

国際出願番号　ＰＣＴ／ＪＰ２００４／０１８４９１

第Ⅰ欄　報告の基礎

1．言語に関し、この予備審査報告は以下のものを基礎とした。

☑ 出願時の言語による国際出願

☐ 出願時の言語から次の目的のための言語である＿＿＿＿＿＿＿＿ 語に翻訳された、この国際出願の翻訳文

- ☐ 国際調査（ＰＣＴ規則12.3(a)及び23.1(b)）
- ☐ 国際公開（ＰＣＴ規則12.4(a)）
- ☐ 国際予備審査（ＰＣＴ規則55.2(a)又は55.3(a)）

2．この報告は下記の出願書類を基礎とした。（法第6条（ＰＣＴ14条）の規定に基づく命令に応答するために提出された差替え用紙は、この報告において「出願時」とし、この報告に添付していない。）

☐ 出願時の国際出願書類

☑ 明細書

第 1, 3-20, 25-33, 35-43, 45-58 ページ、出願時に提出されたもの
第 2, 21-24/1, 34, 44 ページ*、2005.09.20 付けで国際予備審査機関が受理したもの
第 ＿＿＿＿＿＿ ページ*、＿＿＿＿＿＿ 付けで国際予備審査機関が受理したもの

☑ 請求の範囲

第 2-39, 41 項、出願時に提出されたもの
第 ＿＿＿＿＿＿ 項*、ＰＣＴ１９条の規定に基づき補正されたもの
第 1, 40 項*、2006.02.08 付けで国際予備審査機関が受理したもの
第 ＿＿＿＿＿＿ 項*、＿＿＿＿＿＿ 付けで国際予備審査機関が受理したもの

☑ 図面

第 1/33-6/33, 8/33-33/33 ページ/~~図~~、出願時に提出されたもの
第 7/33 ページ/~~図~~*、2005.09.20 付けで国際予備審査機関が受理したもの
第 ＿＿＿＿＿＿ ページ／図*、＿＿＿＿＿＿ 付けで国際予備審査機関が受理したもの

☐ 配列表又は関連するテーブル
配列表に関する補充欄を参照すること。

3．☐ 補正により、下記の書類が削除された。

- ☐ 明細書　第＿＿＿＿＿＿ ページ
- ☐ 請求の範囲　第＿＿＿＿＿＿ 項
- ☐ 図面　第＿＿＿＿＿＿ ページ／図
- ☐ 配列表（具体的に記載すること）＿＿＿＿＿＿
- ☐ 配列表に関連するテーブル（具体的に記載すること）＿＿＿＿＿＿

4．☐ この報告は、補充欄に示したように、この報告に添付されかつ以下に示した補正が出願時における開示の範囲を超えてされたものと認められるので、その補正がされなかったものとして作成した。（ＰＣＴ規則70.2(c)）

- ☐ 明細書　第＿＿＿＿＿＿ ページ
- ☐ 請求の範囲　第＿＿＿＿＿＿ 項
- ☐ 図面　第＿＿＿＿＿＿ ページ／図
- ☐ 配列表（具体的に記載すること）＿＿＿＿＿＿
- ☐ 配列表に関連するテーブル（具体的に記載すること）＿＿＿＿＿＿

＊ 4．に該当する場合、その用紙に "superseded" と記入されることがある。

特許性に関する国際予備報告

国際出願番号 ＰＣＴ／ＪＰ２００４／０１８４９１

第Ｖ欄　新規性、進歩性又は産業上の利用可能性についての法第12条（ＰＣＴ35条(2)）に定める見解、それを裏付ける文献及び説明

1．　見解

新規性（N）　請求の範囲　1 - 41　有
請求の範囲　　無

進歩性（ＩＳ）　請求の範囲　1 - 41　有
請求の範囲　　無

産業上の利用可能性（ＩＡ）　請求の範囲　1 - 41　有
請求の範囲　　無

2．　文献及び説明（ＰＣＴ規則70.7）

文献１：JP 2000-287192 A(株式会社東芝)
文献２：JP 2000-332745 A(三菱電機株式会社)
文献３：JP 2000-59323 A(松下電器産業株式会社)

文献１－３のいずれの文献にも送信装置内でのアクセス位置を示すURIまたは拡張URI情報を用いて、受信装置との間で暗号化または復号化のための認証処理を行うことは記載されていない。

S packet)が複数個集まったものである。TS packetは188byteの固定長パケットで、その長さはATMのセル長との整合性およびリードソロモン符号などの誤り訂正符号化を行なう場合の適用性を考慮して決定されている。TS packetは4byte固定長のパケットヘッダと可変長のアダプテーションフィールド(adaptation field)およびペイロード(payload)で構成される。パケットヘッダにはPID(パケット識別子)や各種のフラグが定義されている。このPIDによりTS packetの種類を識別する。adaptation__fieldとpayloadは、片方のみが存在する場合と両方が存在する場合があり、その有無はパケットヘッダ内のフラグ(adaptation__field__control)により識別できる。adaptation__fieldは、PCR(Program__Clock__Reference)等の情報伝送およびTS packetを188byte固定長にするためのTS packet内でのスタッフィング機能を持つ。また、PCRは27MHzのタイムスタンプで、符号化した時の基準時間を復号器のSTCで再現するためにPCRの値が参照される。MPEG－2のTSでは復号器のSTC(System Time Clock)はPCRによるPLL同期機能を持つ。このPLL同期の動作を安定させるためにPCRの送信間隔は最大0.1msである。映像や音声などの個別ストリームが収められたMPEGのPESパケットは同じPID番号を持つ複数のTS packetのpayloadに分割して伝送する。また、PESパケットの先頭は、TS packetの先頭から開始するように構成される。トランスポートストリームは複数のプログラムを伝送することができるため、ストリームに含まれているプログラムとそのプログラムを構成している映像や音声ストリームなどのプログラムの要素との関係を表すテーブル情報が用いられる。このテーブル情報はPSI(Program Specific Information)と呼ばれ、PAT (Program Association Table)、PMT(Program Map Table)などのテーブルを用いる。PAT、PMTなどのPSIはセクションと呼ばれる単位でTS packetの中のpayloadに配置されて伝送される。PATにはプログラム番号に対応したPMTのPIDなどが指定されており、PMTには対応するプログラムに含まれる映像、音声、付加データおよびPCRのPIDが記述されるため、PATとPMTを参照することにより、ストリームの中から目的のプログラムを構成するTS packetだけを取り出すことができる。TSに関する参考文献としては、例えば、CQ出版社、TECH I Vo.4、「画像&音声圧縮技術のすべて(インターネット／ディジタルテレビ、モ

部405、暗号化データ生成部406、暗号化データ復号部407、受信条件設定管理部408、フレーム化部409およびフレーム受信部410を備える。以下、伝送手順に従って、各構成要素の機能を説明する。

[0076] 送信条件設定管理部404は、AVデータ(送信データ)が入力される端子を示す入力端子情報、AVデータのデータフォーマットを示すデータフォーマット情報及びAVデータの属性を示す属性情報を含むAVデータ情報、具体的には、送信データの種別、送信先アドレスやポート番号の情報、送信に用いるパス情報(ルーティング情報)、送信データの帯域、送信データの送信優先度などの送信条件の設定情報と、送信部(ローカル)と受信部(リモート)における機器の管理制御データと、受信状況を送信側にフィードバックするためのデータを取得し、パケット化部403やフレーム化部409におけるヘッダやペイロードデータなどの生成を制御(パラメータの設定等を)する。

[0077] なお、パケット送受信部401におけるAVデータ(送信データ)が入力される端子を示す入力端子情報とは、例えば取り扱う信号がAVデータがMPEG－TS信号の場合、(1)デジタル放送の入力端子(日本の場合、地上デジタル放送、BSデジタル放送、110度広帯域CSデジタル放送に対応するRF入力端子がある)、(2)IEEE1394 D－I／F、(3)USB－I／F、(4)IP－I／F(Ethernet(登録商標)や無線LANの区別)、(5)アナログ映像音声入力(この場合は、パケット送受信部401内で入力されたアナログ映像音声をMPEG－TS信号に変換する)などがある。なお、デジタル放送に関しては、映像情報メディア学会誌、Vol. 58、No. 5、pp. 604～pp. 654において解説記事がある。

[0078] また、パケット送受信部401におけるAVデータのデータフォーマットを示すデータフォーマット情報とは、例えば取り扱う信号がAVデータがMPEG－TS信号の場合、MPEG－TSのMIME－Typeやメディアフォーマットを表わす。たとえば、送信手段(サーバ)や受信手段(クライアント)が取り扱う静止画メディア、音楽メディア、動画メディアに対して、それぞれのメディアフォーマットを定める。静止画のメディアフォーマットとしては、JPEG、PNG、GIF、TIFFなどがある。また、音楽のメディアフォーマットとしては、リニアPCM、AAC、AC3、ATRAC3plus、MP3、WMAなどがある。ま

た、動画(映像)のメディアフォーマットとしては、MPEG2、MPEG1、MPEG4、WMVなどがある。これらは、たとえば、DLNA(Digital Living Network Alliance；ホームページはwww.dlna.org)でも同様に規定されている。DLNAのversion 1.0では、サーバ(コンテンツの送信側、DTCPではソース)をDMS(Digital Media Server)、クライアント(コンテンツの受信側、DTCPではシンク)をDMP(Digital Media Player)と呼んでいる。DMSはUPnP－AVのMediaServer(MS)とControlPoint(CP)により構成され、DMPはUPnP－AVのMediaRenderer(MR)とControlPoint(CP)により構成される。UPnP－AVのMS, MR、CPについては、UPnPのホームページ、www／upnp.orgに記載されている。

[0079] 映像メディアフォーマットの場合、(1)解像度の区別(SD、HD)、(2)TV方式の区別(アナログではNTSC、PAL, SECAM, デジタルでは米国ATSC、欧州DVB、日本のISDBなどARIB規格に基づく放送方式)、(3)タイムスタンプ形式などの付加情報の有無、などを追加パラメータとして持つ。なお、たとえば映像の場合、MPEG－PSでもMPEG－TSに対してもMIME－Typeは"mpeg／video"であるので、上記の付加情報を用いることにより、よりきめ細かい映像メディアの取り扱い、制御が可能となる。

[0080] デジタル放送に関するARIB規格の概要は、たとえば、松下テクニカルジャーナル2004年2月、Vol. 50、No. 1、7ページから12ページで解説されている。

[0081] また、パケット送受信部401におけるAVデータの属性を示す属性情報とは、例えば取り扱う信号がAVデータが日本における地上デジタル放送システムで放送局より放送され、家庭等の受信機で選局されたMPEG－TS信号(正確には、ARIB標準規格、ARIB STD B21、第9章において、シリアルインタフェースの入出力トランスポートストリームとして規定されているパーシャルトランスポート信号)の場合、その属性情報としては、放送局よりPSI／SI情報として送信される、チャンネル名(放送局名)、チャンネル番号、番組名、番組のジャンル、スケジュールされた放送開始時間、スケジュールされた放送終了時間、番組内容に関する情報、番組の解像度、パレンタルなどの視聴制限情報、コピー制御情報、視聴料金などがある。PSIに関しては、ARIB技術資料、ARIB TR－B14やARIB TR－B15にて規定されている。

[0082] AKE部402は、認証部413と暗号化鍵交換部414を具備する。このAKE部402は、認証と鍵交換に関する設定情報(AKE設定情報)を取得し、このAKE設定情報に関連した情報、たとえば、コピー保護情報と暗号化鍵変更情報をパケット化部403に出力する。

[0083] パケット化部403(403a)は、送信条件設定管理部404から送られてくる送信パラメータに従って、AKE部402から送られてくるAKE設定情報に関連した情報をTCP/IPのヘッダとして付加し、フレーム化部409に送る。

[0084] フレーム化部409は、送信条件設定管理部404から送られてくる送信パラメータに従って、パケット化部403からのIPパケットに対してさらにMACヘッダを付加することで、イーサネット(登録商標)フレームに変換し、送信フレームとしてネットワークに出力する。

[0085] 受信側では、フレーム受信部410は、ネットワークより入力される信号(フレーム)に対して、MACヘッダを元にフィルタリングして受信し、IPパケットとしてパケット受信部405に渡す。

[0086] パケット受信部405(405a)は、フレーム受信部410から送られてくるIPパケットに対して、IPパケットヘッダなどの識別によりフィルタリングを行い、AKE部402に出力する。これにより、送信側のAKE部と、受信側のAKE部がネットワークを介して接続されるので、通信プロトコルを介してお互いにメッセージの交換ができる。すなわち、AKE部の設定手順に従い、認証と鍵交換が行われる。

[0087] 送信側と、受信側で認証と鍵交換が成立すれば、暗号化したAVデータを送信する。

送信側では、MPEG－TS信号が暗号化データ生成部406に入力され、暗号化データ生成部406内の暗号化部411は、MPEG－TS信号を暗号化する。続いて、暗号化情報ヘッダ付加部412は、AKE部402から送られてくる前述したEMIおよびシード情報(シード情報のすべてのビット、または、O/Eなど一部のビット)などのAKE情報を暗号化情報ヘッダとして付加し、パケット化部403に出力する。パケット化部403は、暗号化データ生成部406からのデータに対して、送信条件設定管理部404からの送信条件などのパラメータを用いて、TCP/IPのヘッダを付加し、フレーム化

部409に送る。フレーム化部409は、パケット化部403からのIPパケットに対して、802.1Q(VLAN)方式を用いてMACヘッダを付加することでイーサネット(登録商標)フレームに変換し、送信フレームとしてネットワークに出力する。ここで、MACヘッダ内のTCI(Tag Controal Informaition)内のPriority(ユーザ優先度)を高く設定することにより、ネットワーク伝送の優先度を一般のデータよりも高くすることができる。

[0088] 受信側では、ネットワークより入力される信号がフレーム受信部410でMACヘッダを元にフィルタリングされ、IPパケットとしてパケット受信部405に入力される。パケット受信部405でパケットヘッダなどの識別によりフィルタリングされ、暗号化データ復号部407に入力され、暗号化データ復号部407にて暗号化情報ヘッダの除去と暗号の復号化が行われ、復号されたMPEG－TS信号が出力される。

[0089] なお、送信条件設定管理部404には、受信条件設定管理部408を介して、受信状況を送信側にフィードバックするためのデータが入力され、送信条件設定管理部404において、IPパケットのパケット化部403およびイーサネット(登録商標)フレームのフレーム化部409で生成するヘッダおよびペイロードデータが設定される。

[0090] 次に、図10のプロトコルスタックを用いて上記手順を補足説明する。図10に示された送信側において、まず送信側から受信側へ暗号化されたコンテンツおよびコンテンツの保護モード情報が送信される。受信側は、コンテンツのコピー保護情報の解析を行い、認証方式を決定し、認証要求をパケット送信機器に送る。次に、乱数を発生させ、この乱数を所定の関数に入力し、交換鍵を作成する。交換鍵の情報を所定の関数に入力し、認証鍵を生成する。受信側でも所定の処理により認証鍵の共有を図る。なお、ここで用いる暗号化情報としては、たとえば、送信側の独自情報(機器ID、機器の認証情報、マックアドレスなど)、秘密鍵、公開鍵、外部から与えられた情報などを1つ以上組み合わせて生成した情報であり、DES方式やAES方式など暗号化強度の強い暗号化方式を用いることにより強固な暗号化が可能である。そして、送信側は認証鍵を用いて交換鍵を暗号化して受信側に送り、受信側で交換鍵が復号される。また、交換鍵と初期鍵更新情報を所定の関数に入力し、暗号化鍵を生成する。なお、送信側では暗号鍵を時間的に変化させるために、時間的に変化する鍵更新

情報を生成し、受信側に送信する。コンテンツであるMPEG－TSは暗号化鍵により

暗

205において、時間的に変化するシード情報(O／E)が生成され、DTCP情報生成部1201および第1パケット化部901を経由してシンクに送信される。

(ステップS17)ソースでは、暗号化鍵生成部1205において交換鍵とシード情報より暗号化鍵が生成され、暗号化データ生成部406でMPEG－TSが暗号化され、第2パケット化部902に出力される。

(ステップS18)シンクでは、暗号鍵変更情報生成部1206は、第1パケット受信部903よりシード情報を受信し、復号鍵生成部1207は、このシード情報と交換鍵生成部1204の情報より、復号鍵を復元する。

(ステップS19)シンクでは、この復号鍵を用いて暗号化データ復号部407において、暗号化されたMPEG－TS信号が復号される。

[0124] 図18(a)に示されるように、第1パケット化部901では、入力データは、RTCPまたはRTSP、TCPまたはUDP、さらにIPによる処理がなされ、出力される。なお、RTCP(rfc1889)は、ネットワークの実効帯域幅や遅延時間などを受信装置より送信装置に送り、送信装置は報告された通信状態に合わせてRTPで送信するデータの品質を調整して送信することもできる。また、RTSP(rfc2326)は、再生、停止、早送り、などの制御コマンドを送ることもでき、AVファイルよりデータをダウンロードしながらコンテンツを再生することが可能である。また、第2パケット化部902では、入力データは、RTP、UDP、そしてIPでそれぞれ処理され、IPパケットが出力される。

[0125] 一方、図18(b)に示されるように、第1パケット受信部903では、受信データは、フィルタリングなどIP受信処理、TCPまたはUDPの受信処理、さらに、RTCPまたはRTSPによる受信処理がなされ、データが出力される。また、第2パケット受信部904では、受信データは、フィルタリングなどIP受信処理、UDPの受信処理、さらに、RTPの受信処理がなされ、データが出力される。

[0126] 以上により、パケット送受信機器間でMPEG－TS信号をDTCP方式により暗号化してリアルタイム伝送が可能となるだけでなく、第2パケット化部902がハードウェアで構成されているため、本質的にソフトウェア処理に起因する送信パケットの送り残しや受信パケットの取りこぼしが発生しない。また、データ量の小さい第1パケット化部901はマイコンなど安価なプロセッサで処理できる。

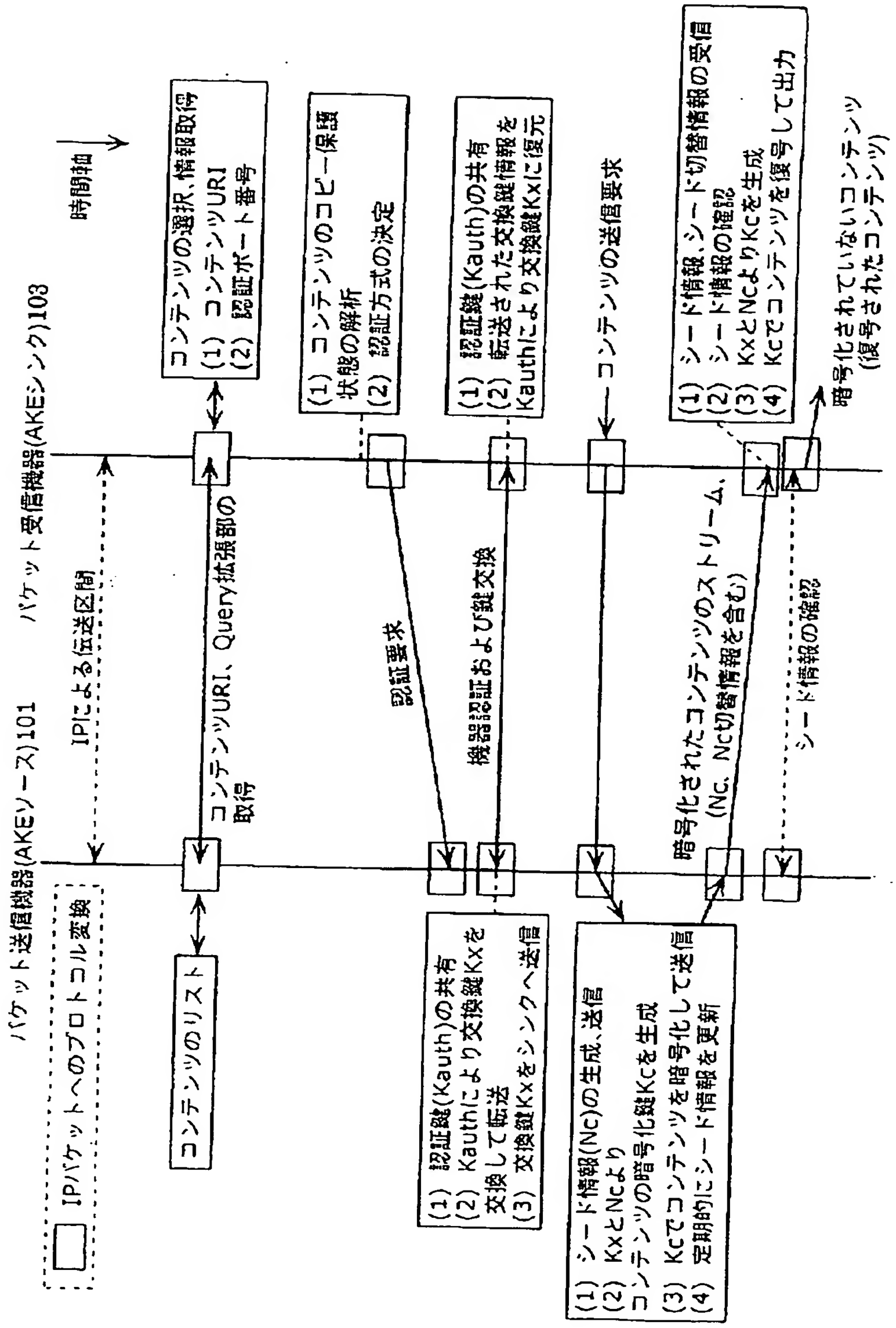
のコピー保護情報の解析を行い、認証方式を決定し、認証要求をパケット送信機器に送る。次に、乱数を発生させ、この乱数を所定の関数に入力し、交換鍵を作成する。交換鍵の情報を所定の関数に入力し、認証鍵を生成する。受信側でも所定の処理により認証鍵の共有を図る。なお、ここで用いる暗号化情報としては、たとえば、送信側の独自情報(機器ID、機器の認証情報、マックアドレスなど)、秘密鍵、公開鍵、外部から与えられた情報などを1つ以上組み合わせて生成した情報であり、DES方式やAES方式など暗号化強度の強い暗号化方式を用いることにより強固な暗号化が可能である。そして、送信側は認証鍵を用いて交換鍵を暗号化して受信側に送り、受信側で交換鍵が復号される。また、交換鍵と初期鍵更新情報を所定の関数に入力し、暗号化鍵を生成する。なお、送信側では暗号鍵を時間的に変化させるために、時間的に変化する鍵更新情報を生成し、受信側に送信する。コンテンツであるMPEG－TSは暗号化鍵により暗号化される。そして暗号化されたMPEG－TSは、AVデータとしてTCP(またはUDP)パケットのペイロードとしてTCPパケットが生成される。さらにこのTCPパケットはIPパケットのデータペイロードとして使用され、IPパケットが生成される。さらにこのIPパケットはMACフレームのペイロードデータとして使用され、イーサネット(登録商標)MACフレームが生成される。なお、MACとしてはイーサネット(登録商標)であるIEEE802．3だけでなく、無線LAN規格のIEEE802．11のMACにも適用できる。

[0167] さて、イーサネット(登録商標)MACフレームは、イーサネット(登録商標)上を送信側から受信側へ伝送される。受信側で所定の手順に従って復号鍵が生成される。そして、受信したイーサネット(登録商標)MACフレームからIPパケットがフィルタリングされる。さらにIPパケットからTCP(またはUDP)パケットが抜き出される。そして、TCP(またはUDP)パケットからAVデータが抜き出され、交換鍵と鍵変更情報より復元された復号鍵により、MPEG－TS(コンテンツ)が復号され出力される。

[0168] 以上、MPEG－TS信号などのAVストリームがパケット送信機器で暗号化され、IPパケットでネットワークにより伝送され、パケット受信機器で元の信号に復号される。

[0169] なお、送信キュー制御部2407は、第1キューとしてのAVデータキュー、および、第2キューとしての一般データキューを具備している。

【図7】



補正された用紙(条約第34条)

PCT/JP2004/018491
日本国特許庁 08.02.06

請求の範囲

[1] (補正後)パケット受信装置にパケットデータを送信するパケット送信装置であって、

ＡＶデータが入力される端子を示す入力端子情報、前記ＡＶデータのデータフォーマットを示すデータフォーマット情報及び前記ＡＶデータの属性を示す属性情報を含むＡＶデータ情報を取得するＡＶデータ情報取得手段と、

前記ＡＶデータ及び非ＡＶデータの入力を受け付けるデータ入力手段と、

前記非ＡＶデータまたは前記ＡＶデータより、前記ＡＶデータの課金情報、再生制御情報及びコピー制御情報の少なくとも１つの情報を抽出し、抽出した情報から、前記ＡＶデータを送信する際の条件となる暗号化モードを示す暗号化モード情報を生成する送信条件設定管理手段と、

前記入力端子情報、前記データフォーマット情報及び前記属性情報を組み合わせて決定される送信条件に基づいて、前記データ入力手段より入力された前記ＡＶデータを暗号化し、暗号化された前記ＡＶデータに対して前記暗号化モード情報に基づく暗号化情報ヘッダを付加することによって暗号化データを生成する暗号化データ生成手段と、

前記暗号化データ生成手段により生成された暗号化データに対して、パケットヘッダを付加することによってパケットを生成するパケット化手段と、

前記ＡＶデータの前記パケット送信装置内でのアクセス位置を示すＵＲＩ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｉｄｅｎｔｉｆｉｅｒ）情報または拡張ＵＲＩ情報を用いて、前記パケット受信装置との間で前記ＡＶデータの暗号化または復号化のための認証処理を行う認証手段と、

前記入力端子情報、前記属性情報及び前記パケット受信装置より指定される送信モードを示す情報の少なくとも１つを用いて、前記パケット送信装置と前記パケット受信装置の間での前記ＡＶデータの伝送プロトコルを決定する伝送プロトコル決定手段と、

前記認証処理によって前記パケット受信装置との認証処理が完了した後に、前記伝送プロトコル決定手段によって決定された伝送プロトコルに従って、前記パケット化手段によって生成された暗号化データを含むパケットを前記パケット受信装置に伝送する伝送手段と

を備えることを特徴とするパケット送信装置。

[2] 前記パケット送信装置はさらに、前記送信条件設定管理手段より入力される前記課

が前記パケット受信装置におけるＣｏｎｎｅｃｔｉｏｎＭａｎａｇｅｒに対して前記ｉｔｅｍに関する論理的接続に関連して設定するＵＰｎＰ－ＡＶ手段のｃｏｎｎｅｃｔｉｏｎＩＤの少なくとも１つを含んでおり、

前記パケット送信装置はさらに、前記パケット受信装置として前記パケット送信装置内の蓄積メディアデバイスのプログラム選択を行なう時に、前記伝送ストリームのｐｒｏｐｅｒｔｙを参照することにより、伝送ストリームに空きあるか無いか、およびどの蓄積メディアデバイスのどのプログラムが選択されているかを判別する受信制御手段を備える

ことを特徴とする請求項３６記載のパケット送信装置。

[３９] 「前記ストリームを伝送するトランスポート層が使用するＴＣＰまたはＵＤＰのポート番号」、および、「前記パケット受信装置におけるＵＰｎＰ－ＡＶ手段のＣｏｎｎｅｃｔｉｏｎＭａｎａｇｅｒが前記パケット送信装置におけるＣｏｎｎｅｃｔｉｏｎＭａｎａｇｅｒに対して前記ｉｔｅｍに関する論理的接続に関連して設定するＵＰｎＰ－ＡＶ手段のｃｏｎｎｅｃｔｉｏｎＩＤ、または前記パケット送信装置におけるＵＰｎＰ－ＡＶ手段のＣｏｎｎｅｃｔｉｏｎＭａｎａｇｅｒが前記パケット受信装置におけるＣｏｎｎｅｃｔｉｏｎＭａｎａｇｅｒに対して前記ｉｔｅｍに関する論理的接続に関連して設定するＵＰｎＰ－ＡＶ手段のｃｏｎｎｅｃｔｉｏｎＩＤ」の論理対により、前記ＵＰｎＰ－ＡＶ手段と、前記ＴＣＰまたは前記ＵＤＰを使用するＨＴＴＰまたはＲＴＰを用いるトランスポート手段とが論理的に対応づけられる

ことを特徴とする請求項１または３７または３８記載のパケット送信装置。

[４０] (補正後)パケット受信装置にパケットデータを送信するパケット送信方法であって、

ＡＶデータが入力される端子を示す入力端子情報、前記ＡＶデータのデータフォーマットを示すデータフォーマット情報及び前記ＡＶデータの属性を示す属性情報を含むＡＶデータ情報を取得するＡＶデータ情報取得ステップと、

前記ＡＶデータ及び非ＡＶデータの入力を受け付けるデータ入力ステップと、

前記非ＡＶデータまたは前記ＡＶデータより、前記ＡＶデータの課金情報、再生制御情報及びコピー制御情報の少なくとも１つの情報を抽出し、抽出した情報から、前記ＡＶデータを送信する際の条件となる暗号化モードを示す暗号化モード情報を生成する送信条件設定管理ステップと、

前記入力端子情報、前記データフォーマット情報及び前記属性情報を組み合わせ

て決定される送信条件に基づいて、前記データ入力ステップで入力された前記ＡＶデータを暗号化し、暗号化された前記ＡＶデータに対して前記暗号化モード情報に基づく暗号化情報ヘッダを付加することによって暗号化データを生成する暗号化データ生成ステップと、

前記暗号化データ生成ステップで生成された暗号化データに対して、パケットヘッダを付加することによってパケットを生成するパケット化ステップと、

前記ＡＶデータの前記パケット送信装置内でのアクセス位置を示すＵＲＩ情報または拡張ＵＲＩ情報を用いて、前記パケット受信装置との間で前記ＡＶデータの暗号化または復号化のための認証処理を行う認証ステップと、

前記入力端子情報、前記属性情報及び前記パケット受信装置より指定される送信モードを示す情報の少なくとも１つを用いて、前記パケット送信装置と前記パケット受信装置の間での前記ＡＶデータの伝送プロトコルを決定する伝送プロトコル決定ステップと、

前記認証処理によって前記パケット受信装置との認証処理が完了した後に、前記伝送プロトコル決定ステップで決定された伝送プロトコルに従って、前記パケット化ステップによって生成された暗号化データを含むパケットを前記パケット受信装置に伝送する伝送ステップと

を含むことを特徴とするパケット送信方法。

[41] パケット受信装置にパケットデータを送信するパケット送信装置のためのプログラムであって、

請求項４０記載のパケット送信方法に含まれるステップをコンピュータに実行させることを特徴とするプログラム。